



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,625	04/28/2006	Audrius Berzanskis	053-03US1	5658
53590 7590 12/16/2008 OPTICUS IP LAW, PLLC 7791 ALISTER MACKENZIE DRIVE SARASOTA, FL 34240			EXAMINER LAFORGLA, CHRISTIAN A	
			ART UNIT 2439	PAPER NUMBER
			MAIL DATE 12/16/2008	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/577,625

**Applicant(s)**

BERZANSKIS ET AL.

**Examiner**

Christian LaForgia

**Art Unit**

2439

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 September 2008.  
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.  
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-13 is/are pending in the application.  
4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.  
6) ☒ Claim(s) 1-13 is/are rejected.  
7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.  
8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☒ The specification is objected to by the Examiner.  
10) ☒ The drawing(s) filed on 28 April 2006 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☒ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)  
2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)  
3) ☒ Information Disclosure Statement(s) (PTO-8508)  
Paper No(s)/Mail Date 5/21/08  
4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_  
5) ☐ Notice of Inventor's Patent Application  
6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

***Continued Examination Under 37 CFR 1.114***

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(c), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(c) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 29 September 2008 has been entered.
2. Claims 1-13 have been presented for examination.

***Response to Arguments***

3. Applicant's arguments, see pages 5-7, filed 29 September 2008, with respect to the specification have been fully considered and are persuasive. The new matter objection of the specification has been withdrawn.
4. Applicant's arguments, see pages 7-9, filed 29 September 2008, with respect to independent claims 1, 5, 8, and 9 have been fully considered and are persuasive. The new matter objection of independent claims 1, 5, 8, and 9 has been withdrawn.
5. Applicant's arguments, see page 10, filed 29 September 2008, with respect to the rejections under 35 U.S.C. 112, 1<sup>st</sup> paragraph have been fully considered and are persuasive. The 35 U.S.C. 112, 1<sup>st</sup> paragraph rejection of claims 1-13 has been withdrawn.
6. Applicant's arguments with respect to claims 1-13 have been considered but are moot in view of the new grounds of rejection set forth below.

***Information Disclosure Statement***

7. The information disclosure statement (IDS) submitted on 21 May 2008 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.
8. The information filed 29 September 2008 fails to comply with 37 CFR 1.98(a)(1), which requires the following: (1) a list of all patents, publications, applications, or other information submitted for consideration by the Office; (2) U.S. patents and U.S. patent application publications listed in a section separately from citations of other documents; (3) the application number of the application in which the information disclosure statement is being submitted on each page of the list; (4) a column that provides a blank space next to each document to be considered, for the examiner's initials; and (5) a heading that clearly indicates that the list is an information disclosure statement. The information has been placed in the application file, but the information referred to therein has not been considered. The information will not be considered until the Applicant files a proper information disclosure statement.

***Claim Rejections - 35 USC § 103***

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.
10. Claims 1 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,757,912 to Blow, hereinafter Blow, in view of U.S. Patent Application Publication No. 2003/0112970 A1 to Mitra, hereinafter Mitra.

Art Unit: 2439

11. As per claim 1, Blow teaches a method of performing quantum key distribution (QKD) (column 7, line 57), comprising a random set of bits that can be used to generate a key (column 10, lines 54-67).

12. Blow does not teach encrypting the key bits and using the encrypted key bits to form encrypted qubits.

13. Mitra discloses encrypting key bits (paragraph 0013) and transmitted the encrypted key bits (paragraphs 0013, 0014, i.e. transmitting either classically or quantum).

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming unencrypted qubits from the optical pulses, since Mitra states at paragraph 0010 that a classical key distribution system provides security against eavesdropping and cheating.

15. As per claim 9, Blow teaches a quantum cryptography system, comprising:

a) a quantum key distribution (QKD) that encodes weak optical pulses to form qubits (column 7, lines 57-67).

16. Blow does not teach key bits and basis bits and a classical encryption system operably coupled to the QKD system and adapted to encode at least one of the key bits and the basis bits to form encrypted qubits.

17. Mitra discloses encrypting key bits (paragraph 0013) and transmitted the encrypted key bits (paragraphs 0013, 0014, i.e. transmitting either classically or quantum).

18. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming

unencrypted qubits from the optical pulses, since Mitra states at paragraph 0010 that a classical key distribution system provides security against eavesdropping and cheating.

19. Claims 2-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blow in view of Mitra as applied above, and further in view of **Applied Cryptography**, to Bruce Schneier, hereinafter Schneier.

20. Regarding claim 2, Blow and Mitra do not teach encrypting the key bits using a stream cipher.

21. Schneier teaches the use of stream ciphers (pages 197-211).

22. One of ordinary skill in the art could have combined a stream cipher in the combined system of Blow and Mitra since Schneier discloses at page 197 that stream ciphers convert plaintext to ciphertext one bit at a time. This would have been the most practical solution since the Applicant is breaking the key into bits, Blow discloses a combination of secret bits used to formulate a key, and Mitra encrypts the data bit by bit to form quantum bits (aka qubits). See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

23. With regards to claim 3, Blow, Mitra, and Schneier do not teach the use of a password.

24. The Examiner takes Official Notice that the use of passwords is well-known and commonly practiced in the art and one of ordinary skill in the art would clearly recognize the benefits and motivation for using a password.

25. With regards to claim 4, Mitra teaches decoding the encrypted bits on the receiving side (paragraph 0013). Schneier discloses the use of stream ciphers (pages 197-211).

26. As per claim 5, Blow teaches a method of performing quantum key distribution (QKD) (column 7, line 57) comprising a first QKD station that generates a random set of bits that can be used to generate a key (column 10, lines 54-67).

27. Schneier teaches generating a key stream using a key stream generator and then XORing that data to the plain text data to produce the stream of ciphertext bits (page 197).

28. One of ordinary skill in the art could have combined generate a pad (aka key stream) and XOR the pad with the key bits since Schneier discloses at page 197 that stream ciphers convert plaintext to ciphertext one bit at a time. This would have been the most practical solution since the Applicant is breaking the key into bits and Blow discloses a combination of secret bits used to formulate a key. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

29. Blow and Schneier do not teach modulating weak optical pulses using the encrypted key bits to generate encrypted qubits.

30. The Applicant admits in the "Background Art" section of the specification that quantum key distribution involves establishing a key between a sender and receiver utilizing weak optical signals (page 2, Amendment to the Specification, 4/28/06). Since all of the references deal with quantum communications they all involved weak optical signals.

31. Mitra discloses encrypting key bits (paragraph 0013) and transmitted the encrypted key bits (paragraphs 0013, 0014, i.e. transmitting either classically or quantum).

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming unencrypted qubits from the optical pulses, since Mitra states at paragraph 0010 that a classical key distribution system provides security against eavesdropping and cheating.

33. Regarding claim 6, "Quantum Cryptography: Public Key Distribution and Coin Tossing" to C.H. Bennett et al., hereinafter Bennett, discloses that Bob (the receiver) decides randomly for each photon received whether to measure the photon rectilinear polarization or diagonal polarization (see Section III, page 3, first paragraph).

34. Mitra teaches decoding the encrypted qubits on the receiving side (paragraph 0013). Schneier discloses the use of stream ciphers, specifically XORs to encrypt/decrypt a stream (pages 197-211).

35. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blow in view of Mitra as applied above, and in further view of U.S. Patent Application Publication No. 2002/0106084 A1 to Azuma et al., hereinafter Azuma.

36. With regards to claim 7, Blow and Mitra do not teach establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station.

37. Azuma teaches establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD

station (paragraph 0007, i.e. results obtained from the observation bases on the Alice and Bob sides that match are adopted as data).

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to establish a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station, since Azuma states at paragraph 0049 that establishing a sifted key prevents an eavesdropper from extracting the original data even if the quantum state was stolen.

39. Claims 8-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend, hereinafter Townsend, in view of U.S. Patent Application Publication No. 2006/0120529 A1 to Gisin et al., hereinafter Gisin, and further in view of Schneier in view of Mitra.

40. As per claim 8, Townsend teaches a QKD system, comprising:

a) a first QKD station (Figure 4 [block 1]) having:

a. an optical radiation source adapted to emit weak optical pulses of radiation (Figure 4 [block 48], column 4, lines 34-48, column 6, lines 41-63);

d. a modulator arranged to receive the weak optical pulses and adapted to modulate the polarization or phase of the weak optical pulses based on the encrypted key bits to form encrypted qubits (Figure 4 [block 49], column 4, lines 34-55);

b) a second QKD station (Figure 4 [block 2]) optically coupled to the first QKD station (Figure 4 [block 3]) and having:

a. a second modulator adapted to receive and randomly polarization-modulate or phase-modulate the encrypted qubits (Figure 4 [block 52], column 4, lines 34-55, column 6, lines 41-63);

b. a detector for detecting the modulated encrypted qubits (Figure 2 [block 10], column 6, lines 1-40).

41. Townsend does not teach a first random number generator adapted to generate random numbers for use as first key bits.

42. Gisin teaches the use of a random number generator to prepare random quantum states (Figure 1 [blocks 14, 44], paragraph 0026, claim 7).

43. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a random number generator to generate random numbers for the key bits, since Schneier states at page 197 that a randomized key stream allows for perfect security since patterns and strings of similar numbers can result in the key being determined by an eavesdropper.

44. Townsend and Gisin do not teach a first e/d module coupled to the first random number generator to encrypt the key bits thereby forming encrypted key bits and a second e/d module coupled to the detector and adapted to recover from the modulated encrypted qubits second key bits corresponding to the first key bits.

45. Mitra discloses encrypting key bits (paragraph 0013) and transmitted the encrypted key bits (paragraphs 0013, 0014, i.e. transmitting either classically or quantum).

46. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming

unencrypted qubits from the optical pulses, since Mitra states at paragraph 0010 that a classical key distribution system provides security against eavesdropping and cheating.

47. Regarding claim 10, Schneier teaches wherein classical encryption system includes an encryption/decryption (e/d) module configured to perform XOR-ing of the key bits and a password to form encrypted key bits (page 197).

48. Regarding claim 11, Schneier teaches wherein the classical encryption system is adapted to generate the password using a stream cipher (page 197).

49. With regards to claim 12, Townsend teaches a phase modulator operably coupled to the classical encryption system and configured to impart a phase to each weak optical pulse based on one of said encrypted key bits (Figures 1 [elements 100, 102], 2, column 3, line 26-67).

50. Concerning claim 13, Townsend teaches wherein the basis bits are encoded, and wherein the phase modulator is configured to encode each weak optical pulse with one of the encoded basis bits (Figures 1 [elements 100, 102], 2, column 3, line 26-67).

### *Conclusion*

51. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

52. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

53. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/  
Primary Examiner, Art Unit 2439

clf